SECURITY BREACHES

Have you received a letter informing you that your personal information may have gotten into the wrong hands? It is increasingly common for companies, educational institutions, and government agencies (whether or not their state has a breach notice law) to notify individuals when computer files containing personal information have been hacked, stolen, or lost. If the file includes your SSN, financial account numbers, driver's license numbers, or data that would be useful to identity thieves, there are steps you can take to reduce your risk of fraud.

What should you do if you receive a letter telling you that your personal information has been compromised?
First, don't panic. A security breach does not necessarily mean that you will become a victim of identity theft.

1. Figure out what type of breach has occurred. Has a breach occurred with your *existing* financial account? Has your SSN been compromised, with the chance that *new accounts* can be established by an imposter? Has your driver's license number been compromised, or another government-issued ID document?

- **Existing accounts.** If the breach involved your *existing* credit or debit card account, you will want to monitor your monthly account statements very carefully. Contact the creditor if your statement does not arrive on time. A missing bill could mean that an identity thief has changed your address. Check statements for transactions you did not make. Dispute those fraudulent charges directly with the credit or debit card company. The company will likely cancel the account and give you a new card and account number. You will not be responsible for the fraudulent charges if you properly dispute them. It's very important to report the fraudulent transactions immediately. In some situations, the financial company will not wait for evidence of fraud. It will instead cancel the existing account and issue a new account number right away.
- **The potential for new accounts to be opened**. If the breach involved disclosure of your SSN, a fraudster could use that information to open *new accounts* in your name. You will not immediately know of the new accounts because criminals usually use an address other than your own for the account. Since you will not be receiving the monthly account statements, you are likely to be unaware of the account(s). That is why it is so important to place a fraud alert with the three credit reporting agencies immediately when you learn that your SSN has been compromised, and then to monitor your credit reports on an ongoing basis. Other evidence of

SOUTH DAKOTA OFFICE OF ATTORNEY GENERAL
CONSUMER PROTECTION
1302 E Hwy 14 Ste 3 • Pierre SD 57501 consumerhelp@state.sd.us
1-800-300-1986

new account fraud include receiving credit cards in the mail that you did not apply for, being denied credit when you know you've had a good credit score, and being contacted by debt collectors for payments that you do not owe.

- **ID Documents.** Nearly all the security breaches reported to date have potentially involved financial accounts. But if you are notified of a breach involving your driver's license or another government document, contact the agency that issued the document and find out what it recommends in such situations. You might be instructed to cancel the document and obtain a replacement, or the agency might instead "flag" your file to prevent an imposter from getting a license in your name.

2. For security breach situations involving your Social Security Number (SSN) — in other words, breaches in which there is an opportunity for new accounts to be opened in your name you should consider taking the following actions:

- **Notify the credit reporting agencies and establish a fraud alert.** Immediately call the fraud department of one of the three credit reporting agencies — Experian, Equifax, or TransUnion. As soon as the agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.
- **Order your credit reports.** If you are a victim of identity theft, you will see evidence of it on your credit report. Surveys have found that the sooner individuals learn of the identity theft, the more quickly they can clean up their credit reports and regain their financial health.
- **Examine your credit reports carefully**. When you receive your credit reports, look for signs of fraud such as credit accounts that are not yours. Check if there are numerous inquiries on your credit report. If a thief is attempting to open up several accounts, an inquiry will be listed on your credit report for each of those attempts. Usually identity thieves do not succeed in opening all of the accounts that they apply for, only some. Multiple inquiries that you yourself have not generated are a sign of potential fraud. Also, check that your SSN, address(es), phone number(s), and employment information are correct.
- **If your credit report indicates you are a victim of identity theft, you will want to immediately take steps to remove the fraudulent accounts**. If you are a victim you may contact the Federal Trade Commission or the SD Office of Attorney General website for step-by-step information on what you should do.
- **Contact Social Security Administration at 1-800-772-1213.** Do this to verify earnings reported to your social security number and to request a copy of your Social Security Statement.
- **Continue to monitor your credit reports.** Be aware that these measures may not entirely stop new fraudulent accounts from being opened by an imposter. Credit issuers do not always pay attention to fraud alerts. Once you have received the first free copy of your credit report, follow up in a few months and order another.
- **Consider a security freeze.** The three credit reporting agencies — Equifax, Experian, and TransUnion, offer security freezes nationwide.